0011243513
WPI ACC NO: 2002-183303/
XRPX Acc No: N2002-139489

Communication condition control method in internet, involves canceling data transmitted to server, when measured amount of data exceeds preset regulation value

Patent Assignee: NTT COMMUNICATIONS KK (NITE)
Inventor: AIHARA T

1 patents, 1 countries

Patent Family

Patent Number	Kind	Date	Application Number	Kind	Date	Update	
JP 2002016633	A	20020118	JP 2000199565	A	20000630	200224	B

Priority Applications (no., kind, date): JP 2000199565 A 20000630

Patent Details

Number	Kind	Lan	Pg	Dwg	Filing Notes
JP 2002016633	A	JA	10	6	

Alerting Abstract JP A

NOVELTY - A user's server is connected to circuit router through internet. The quantity of data transmitted to the server from the transmitting element having specific IP address, is measured. When measured amount of data exceeds preset regulation value, the data transmitted to the server is canceled.

DESCRIPTION - An INDEPENDENT CLAIM is also included for communication condition control system.

USE - For controlling communication between individual and enterprise through internet.

ADVANTAGE - User's server connected to ISP can be protected from irregular access, by canceling the data being transmitted for more than fixed quantity in ISP.

DESCRIPTION OF DRAWINGS - The figure shows the block diagram of communication condition control system. (Drawing includes non-English language text).

Basic Derwent Week: *200224*

(19)日本国特許庁（ＪＰ）　(12)**公開特許公報（Ａ）**　(11)特許出願公開番号
特開2002－16633
（P2002－16633A）
(43)公開日　平成14年１月18日(2002.1.18)

(51)Int.Cl.'	識別記号	ＦＩ	ﾃｰﾏｺｰﾄﾞ(参考)
Ｈ０４Ｌ　12/56		Ｈ０４Ｌ　11/20	１０２Ｅ　５Ｋ０３０

審査請求　未請求　請求項の数13　ＯＬ　（全 10 頁）

(21)出願番号　特願2000－199565(P2000－199565)

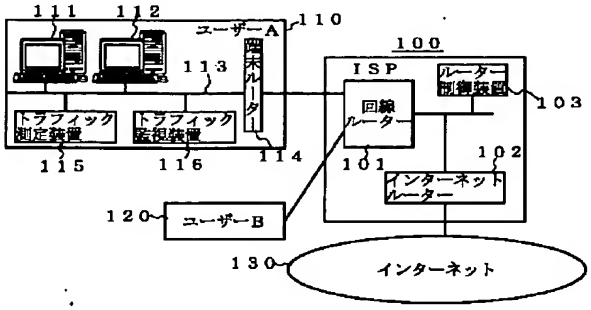
(22)出願日　平成12年６月30日(2000.6.30)

(71)出願人　399035766
エヌ・ティ・ティ・コミュニケーションズ株式会社
東京都千代田区内幸町一丁目１番６号
(72)発明者　相原　俊幸
東京都千代田区内幸町一丁目１番６号　エヌ・ティ・ティ・コミュニケーションズ株式会社内
(74)代理人　100064621
弁理士　山川　政樹

Ｆターム(参考)　5K030 GA13 HD03 HD08 LC11 LC15 MB09

(54)【発明の名称】　通信状態制御方法および通信状態制御システム

(57)【要約】
【課題】　大量のデータを送信してくる不正アクセスから、ＩＳＰに接続されているユーザーのサーバーを守る。
【解決手段】　トラフィック測定装置１１５は、ネットワーク１１３の状態を監視し、トラフィック監視装置１１６が、監視の結果検出された輻輳状態などを判定してルーター制御装置１０３に通知する。また、トラフィック監視装置１１６からの通知により、ルーター制御装置１０３は、回線ルーター１０１やインターネットルーター１０２を制御し、ルーター制御装置１０３から通知されたＩＰアドレスからのデータを破棄させる。



1

【特許請求の範囲】

【請求項１】　インターネット側に接続したインターネットルーターと、このインターネットルーターに接続する回線ルーターとを備えたインターネットサービスプロバイダを介し、ユーザーのサーバーを専用線で前記回線ルーターに接続して前記サーバーを前記インターネットに接続し、

前記サーバーに対して前記インターネットを介して送信されたデータの量と、このデータを送信してきた送信元のＩＰアドレスとを所定時間毎に測定し、

測定したデータ量が予め設定されている規定値以上となった場合、規定値以上のデータ量を送信してきた特定送信元の特定ＩＰアドレスから前記サーバーに対して送信されてきたデータは、前記インターネットルーターまたは前記回線ルーターのいずれか一方もしくは両方に破棄させることを特徴とする通信状態制御方法。

【請求項２】　請求項１記載の通信状態制御方法において、

前記サーバーに対して前記インターネットを介して送信されたデータの量と、このデータを送信してきた送信元のＩＰアドレスとの測定は、前記ユーザー側で行い、

前記ユーザー側で測定したデータ量が予め設定されている規定値以上になったと判断されたとき、前記インターネットサービスプロバイダ側で前記特定ＩＰアドレスから前記サーバーに対して送信されてきたデータを、前記インターネットルーターまたは前記回線ルーターのいずれか一方もしくは両方に破棄させることを特徴とする通信制御方法。

【請求項３】　インターネット側に接続したインターネットルーターと、このインターネットルーターに接続する回線ルーターとを備えたインターネットサービスプロバイダを介し、ユーザーのサーバーを専用線で前記回線ルーターに接続して前記サーバーを前記インターネットに接続し、

前記サーバーのＣＰＵの稼働率とこのＣＰＵの主メモリの使用率と前記サーバーに対する一定時間あたりの総リクエスト数と単位時間あたりの通信量とを測定し、

前記稼働率と使用率と総リクエスト数と通信量とが予め設定されている規定値以上となった場合、規定値以上となった時点においてデータを送信していた特定送信元の特定ＩＰアドレスから前記サーバーに対して送信されてきたデータは、前記インターネットルーターまたは前記回線ルーターのいずれか一方もしくは両方に破棄させることを特徴とする通信状態制御方法。

【請求項４】　請求項３記載の通信状態制御方法において、

前記サーバーのＣＰＵの稼働率とこのＣＰＵの主メモリの使用率と前記サーバーに対する一定時間あたりの総リクエスト数と単位時間あたりの通信量とを測定は、前記ユーザー側で行い、

2

前記ユーザー側で前記稼働率と使用率と総リクエスト数と通信量とが予め設定されている規定値以上になったと判断されたとき、前記インターネットサービスプロバイダ側で前記特定ＩＰアドレスから前記サーバーに対して送信されてきたデータを、前記インターネットルーターまたは前記回線ルーターのいずれか一方もしくは両方に破棄させることを特徴とする通信制御方法。

【請求項５】　請求項１～４いずれか１項記載の通信状態制御方法において、

前記サーバーは、このサーバーが接続するネットワークを介して前記専用線に接続し、前記ネットワークは端末ルーターを介して前記専用線に接続することを特徴とする通信状態制御方法。

【請求項６】　請求項１～５いずれか１項に記載の通信状態制御方法において、

前記インターネットルーターまたは前記回線ルーターのいずれか一方もしくは両方で破棄するデータ量が予め設定されている規定値以下となった場合、前記インターネットルーターまたは前記回線ルーターのいずれか一方もしくは両方における前記特定ＩＰアドレスから前記サーバーに対して送信されたデータの破棄を停止することを特徴とする通信状態制御方法。

【請求項７】　インターネット側に接続されたインターネットルーター、このインターネットルーターに接続された回線ルーター、前記インターネットルーターおよび回線ルーターに接続されて前記インターネットルーターおよび回線ルーターを制御するルーター制御装置を備えたインターネットサービスプロバイダと、

前記回線ルーターに専用線で接続されたユーザーのサーバーと、

このサーバーに対して前記インターネットを介して送信されたデータの量と、このデータを送信してきた送信元のＩＰアドレスとを所定時間毎に測定するトラフィック測定装置と、

このトラフィック測定装置が測定したデータ量を監視してこのデータ量が予め設定されている規定値以上となった場合、規定値以上のデータ量を送信してきた特定送信元の特定ＩＰアドレスを前記ルーター制御装置に通知するトラフィック監視装置とを備え、

前記ルーター制御装置は、前記トラフィック監視装置から通知された特定ＩＰアドレスから前記サーバーに対して送信されてきたデータを、前記インターネットルーターまたは前記回線ルーターのいずれか一方もしくは両方に破棄させるように制御することを特徴とする通信状態制御システム。

【請求項８】　インターネット側に接続されたインターネットルーター、このインターネットルーターに接続された回線ルーター、前記インターネットルーターおよび回線ルーターに接続されて前記インターネットルーターおよび回線ルーターを制御するルーター制御装置を備え

たインターネットサービスプロバイダと、
前記回線ルーターに専用線で接続するユーザーのサーバーと、
このサーバーのＣＰＵの稼働率とこのＣＰＵの主メモリの使用率と前記サーバーに対する一定時間あたりの総リクエスト数と単位時間あたりの通信量とを測定するトラフィック測定装置と、
前記稼働率と使用率と総リクエスト数と通信量とを監視してこれらが予め設定されている規定値以上となった場合、規定値以上となった時点においてデータを送信していた特定送信元の特定ＩＰアドレスを前記ルーター制御装置に通知するトラフィック監視装置とを備え、
前記ルーター制御装置は、前記トラフィック監視装置から通知された特定ＩＰアドレスから前記サーバーに対して送信されてきたデータを前記インターネットルーターまたは前記回線ルーターのいずれか一方もしくは両方に破棄させるように制御することを特徴とする通信状態制御システム。

【請求項９】　請求項７または８記載の通信状態制御システムにおいて、
前記サーバーが接続するネットワークと、
このネットワークと前記専用線とを接続する端末ルーターとを備えたことを特徴とする通信状態制御システム。

【請求項１０】　請求項７～９いずれか１項に記載の通信状態制御システムにおいて、
前記ルーター制御装置は、前記インターネットルーターまたは前記回線ルーターのいずれか一方もしくは両方で破棄するデータ量が予め設定されている規定値以下となった場合、前記インターネットルーターまたは前記回線ルーターのいずれか一方もしくは両方における前記特定ＩＰアドレスから前記サーバーに対して送信されたデータの破棄を停止するように制御することを特徴とする通信状態制御システム。

【請求項１１】　ユーザー側のネットワークに対してトラヒックを渡す回線ルータと、この回線ルータと通信ネットワークを介して接続されてインターネットからの前記ユーザー側のネットワークへのトラヒックを受け取るインターネットルータとを有するネットワークにおける通信状態制御方法であって、
前記ユーザー側のネットワークから、特定のＩＰアドレスからのトラヒックについての制御指示を受け取ると、
前記ユーザーに対応付けて予め登録してある制御内容にしたがって前記回線ルータとインターネットルータとに対してトラヒック配送の制御を行わせることを特徴とする通信状態制御方法。

【請求項１２】　請求項１１記載の通信状態制御方法において、
前記ユーザー側のネットワークからの制御信号は、前記ユーザー側のネットワークが受け取るトラフィック量が予め定めた閾値を越えた際に発せられるものであること

を特徴とする通信状態制御方法。

【請求項１３】　請求項１１記載の通信状態制御方法において、
前記ユーザー側のネットワークからの制御指示は、前記ユーザー側のネットワーク内に設置されたサーバーのシステム稼働率が予め定められた閾値を越えた際に発せられたものであることを特徴とする通信状態制御方法。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、インターネットサービスプロバイダを介してインターネットに接続するときの通信状態制御方法および通信状態制御システムに関する。

【０００２】

【従来の技術】インターネットにおいて、個人や企業がＷｅｂサーバーなど公開サーバーを運用する場合、インターネットサービスプロバイダ（ＩＳＰ：Internet Service Provider）を介して、自身のネットワークをインターネットに接続するようにしている。このＩＳＰによるインターネットへの接続に関して説明すると、図６に示すように、まず、ＩＳＰ６００は、回線ルーター６０１とインターネットルーター６０２とルーター制御装置６０３とを備えている。回線ルーター６０１には、ＩＳＰ６００を利用してインターネットに接続しようとするユーザーＡ６１０，ユーザーＢ６２０からの回線が接続され、インターネットルーター６０２は、インターネット６３０に接続される。

【０００３】一方、ユーザーＡ６１０は、ホームページのＨＴＭＬなどが格納されたＷｅｂサーバー６１１や、メールサーバー６１２などを備え、これらをネットワーク６１３に接続している。ユーザーＡ６１０は、ネットワーク６１３に端末ルーター６１４を設け、回線６４１を介してＩＳＰ６００の回線ルーター６０１に接続している。この構成では、インターネット６３０に接続している他端末６５０とユーザーＡ６１０のＷｅｂサーバー６１１は、端末ルーター６１４－回線ルーター６０１－インターネットルーター６０２の経路で、インターネット６３０を介して接続された状態となる。これらは、ユーザーＢ６２０も同様である。したがって、例えば、他端末６５０からは、Ｗｅｂサーバー６１１に用意されたホームページが閲覧可能な状態となっている。

【０００４】

【発明が解決しようとする課題】ところで、インターネット６３０に接続している他の端末から、ユーザーＡ６１０のＷｅｂサーバー６１１やメールサーバー６１２に対してデータが送信されてくると、返信のためのデータ送信などの応答処理を行う。ところが、上記他の端末から、これらサーバーが処理しきれない大量のデータを送信してくると、Ｗｅｂサーバー６１１やメールサーバー６１２は、対応処理が追いつかず、各サーバー内やネッ

トワーク６１３が輻輳状態となる。従来では、このような不正アクセスが発生した場合、ユーザー側で送信されてきたデータに対する応答を停止するなど、ユーザー側のネットワーク内部で対応してきた。このため、上記ネット攻撃が発生すると、ユーザー側では、ネットワークの輻輳による各サーバーの停止状態を抑制できない場合が多かった。

【０００５】本発明は、以上のような問題点を解消するためになされたものであり、大量のデータを送信してくる不正アクセスから、ＩＳＰに接続されているユーザーのサーバーを守ることを目的とする。

【０００６】

【課題を解決するための手段】本発明の通信状態制御方法は、インターネットサービスプロバイダを介してインターネットに接続しているユーザーのサーバーに対してインターネットを介して送信されたデータの量と、このデータを送信してきた送信元のＩＰアドレスとを所定時間毎に測定し、測定したデータ量が予め設定されている規定値以上となった場合、規定値以上のデータ量を送信してきた特定送信元の特定ＩＰアドレスからサーバーに対して送信されてきたデータは、インターネットルーターまたは回線ルーターのいずれか一方もしくは両方に破棄させようとしたものである。この発明によれば、規定値以上のデータ量を送信してきた送信元からのデータは、ユーザーのサーバーにまで到達しない。

【０００７】上記発明では、サーバーに対してインターネットを介して送信されたデータの量と、このデータを送信してきた送信元のＩＰアドレスとの測定は、ユーザー側で行い、ユーザーで測定したデータ量が予め設定されている規定値以上になったと判断されたとき、インターネットサービスプロバイダ側で特定ＩＰアドレスからサーバーに対して送信されてきたデータを、インターネットルーターまたは回線ルーターのいずれか一方もしくは両方に破棄させる。

【０００８】また、本発明の通信状態制御方法は、インターネットサービスプロバイダを介してインターネットに接続しているユーザーのサーバーのＣＰＵの稼働率とこのＣＰＵの主メモリの使用率とサーバーに対する一定時間あたりの総リクエスト数と単位時間あたりの通信量とを測定し、稼働率と使用率と総リクエスト数と通信量とが予め設定されている規定値以上となった場合、規定値以上となった時点においてデータを送信していた特定送信元の特定ＩＰアドレスからサーバーに対して送信されてきたデータは、インターネットルーターまたは回線ルーターのいずれか一方もしくは両方に破棄させようとしたものである。この発明によれば、測定値が規定値以上となった場合の送信元からのデータは、ユーザーのサーバーにまで到達しない。

【０００９】上記発明では、サーバーのＣＰＵの稼働率とこのＣＰＵの主メモリの使用率とサーバーに対する一定時間あたりの総リクエスト数と単位時間あたりの通信量とを測定は、ユーザー側で行い、ユーザー側で稼働率と使用率と総リクエスト数と通信量とが予め設定されている規定値以上になったと判断されたとき、インターネットサービスプロバイダ側で特定ＩＰアドレスからサーバーに対して送信されてきたデータを、インターネットルーターまたは回線ルーターのいずれか一方もしくは両方に破棄させる。

【００１０】また、上記発明において、サーバーは、このサーバーが接続するネットワークを介して専用線に接続し、ネットワークは端末ルーターを介して専用線に接続する。また、インターネットルーターまたは回線ルーターのいずれか一方もしくは両方で破棄するデータ量が予め設定されている規定値以下となった場合、インターネットルーターまたは回線ルーターのいずれか一方もしくは両方における特定ＩＰアドレスからサーバーに対して送信されたデータの破棄を停止する。

【００１１】本発明の通信状態制御システムは、インターネットルーターおよび回線ルーターに接続されてインターネットルーターおよび回線ルーターを制御するルーター制御装置を備えたインターネットサービスプロバイダと、回線ルーターに専用線で接続されたユーザーのサーバーと、このサーバーに対してインターネットを介して送信されたデータの量と、このデータを送信してきた送信元のＩＰアドレスとを所定時間毎に測定するトラフィック測定装置と、このトラフィック測定装置が測定したデータ量を監視してこのデータ量が予め設定されている規定値以上となった場合、規定値以上のデータ量を送信してきた特定送信元の特定ＩＰアドレスをルーター制御装置に通知するトラフィック監視装置とを備え、ルーター制御装置は、トラフィック監視装置から通知された特定ＩＰアドレスからサーバーに対して送信されてきたデータを、インターネットルーターまたは回線ルーターのいずれか一方もしくは両方に破棄させるように制御するものである。この発明によれば、規定値以上のデータ量を送信してきた送信元からのデータは、ユーザーのサーバーにまで到達しない。

【００１２】本発明の通信状態制御システムは、インターネットルーターおよび回線ルーターに接続されてインターネットルーターおよび回線ルーターを制御するルーター制御装置を備えたインターネットサービスプロバイダと、回線ルーターに専用線で接続するユーザーのサーバーと、このサーバーのＣＰＵの稼働率とこのＣＰＵの主メモリの使用率とサーバーに対する一定時間あたりの総リクエスト数と単位時間あたりの通信量とを測定するトラフィック測定装置と、稼働率と使用率と総リクエスト数と通信量とを監視してこれらが予め設定されている規定値以上となった場合、規定値以上となった時点においてデータを送信していた特定送信元の特定ＩＰアドレスをルーター制御装置に通知するトラフィック監視装置

とを備え、ルーター制御装置は、トラフィック監視装置から通知された特定ＩＰアドレスからサーバーに対して送信されてきたデータを、インターネットルーターまたは回線ルーターのいずれか一方もしくは両方に破棄させるように制御するものである。この発明によれば、測定値が規定値以上となった場合の送信元からのデータは、ユーザーのサーバーにまで到達しない。

【００１３】上記発明では、サーバーが接続するネットワークと、このネットワークと専用線とを接続する端末ルーターとを備えている。また、ルーター制御装置は、インターネットルーターまたは回線ルーターのいずれか一方もしくは両方で破棄するデータ量が予め設定されている規定値以下となった場合、インターネットルーターまたは回線ルーターのいずれか一方もしくは両方における特定ＩＰアドレスからサーバーに対して送信されたデータの破棄を停止するように制御する。

【００１４】また、本発明の通信状態制御方法は、ユーザー側のネットワークに対してトラヒックを渡す回線ルータと、この回線ルータと通信ネットワークを介して接続されてインターネットからのユーザー側のネットワークへのトラヒックを受け取るインターネットルータとを有するネットワークにおける通信状態制御方法であって、ユーザー側のネットワークから、特定のＩＰアドレスからのトラヒックについての制御指示を受け取ると、ユーザーに対応付けて予め登録してある制御内容にしたがって回線ルータとインターネットルータとに対してトラヒック配送の制御を行わせようとしたものである。この発明によれば、規定値以上のトラヒックが発生した場合、これの送信元からのデータは、回線ルータとインターネットルータとで制限される。

【００１５】上記発明において、ユーザー側のネットワークからの制御信号は、ユーザー側のネットワークが受け取るトラフィック量が予め定めた閾値を越えた際に発せられるものである。また、ユーザー側のネットワークからの制御指示は、ユーザー側のネットワーク内に設置されたサーバーのシステム稼働率が予め定められた閾値を越えた際に発せられたものである。

【００１６】

【発明の実施の形態】以下、本発明の実施の形態について図を参照して説明する。図１は、本発明の実施の形態における通信状態制御システムの構成を示す構成図である。図１に示すように、まず、ＩＳＰ１００は、回線ルーター１０１とインターネットルーター１０２とルーター制御装置１０３とを備えている。回線ルーター１０１には、ＩＳＰ１００を利用してインターネットに接続しようとするユーザーＡ１１０，ユーザーＢ１２０からの回線が接続され、インターネットルーター１０２は、インターネット１３０に接続される。

【００１７】一方、ユーザーＡ１１０は、ホームページのＨＴＭＬなどが格納されたＷｅｂサーバー１１１やメールサーバー１１２などを備え、これらをネットワーク１１３に接続している。また、ユーザーＡ１１０は、端末ルーター１１４を介し、ネットワーク１１３をＩＳＰ１００すなわち回線ルーター１０１に接続している。したがって、Ｗｅｂサーバー１１１やメールサーバー１１２は、ＩＳＰ１００を介してインターネット１３０に接続した状態となっている。加えて、ユーザーＡ１１０は、トラフィック測定装置１１５とトラフィック監視装置１１６とを備えるようにした。なお、ユーザーＢ１２０も同様である。

【００１８】本実施の形態では、まず、トラフィック測定装置１１５が、ネットワーク１１３の状態を監視し、トラフィック監視装置１１６が、監視の結果検出された輻輳状態などを判定してルーター制御装置１０３に通知するようにした。また、トラフィック監視装置１１６からの通知により、ルーター制御装置１０３が、回線ルーター１０１やインターネットルーター１０２を制御し、ルーター制御装置１０３から通知されたＩＰアドレスからのデータを破棄させるようにした。なお、上記制御により、通知されたＩＰアドレスからのデータをユーザーＡ１１０に送らないように制御してもよく、また、通知されたＩＰアドレスからのデータは、データ量を削減してユーザーＡ１１０側に配送するようなどのように、各ルーターに対してトラヒック配送の制御を行わせるようにしてもよい。

【００１９】詳細に説明すると、まず、トラフィック測定装置１１５は、ネットワーク１１３を通過するデータの発信元ＩＰアドレスと発信先ＩＰアドレスとデータ量とを、所定の時間毎に測定する。例えば、図２に示すように、２秒毎に上記内容を測定し、ＩＰアドレスが「１０．ＸＸ．ＸＸ．ＸＸ」のＷｅｂサーバー１１１に対して送信されたデータ量と，このデータの送信元のＩＰアドレス「２２３．○○．○○．○○」とを検出する。

【００２０】トラフィック監視装置１１６では、トラフィック測定装置１１５が検出した結果の中で、データ量が設定されている値より大きい場合、ユーザーＡ１１０のＷｅｂサーバー１１１がネット攻撃を受けていると判断する。トラフィック監視装置１１６は、ネット攻撃と判断したら、ルーター制御装置１０３に、ＩＰアドレス「２２３．○○．○○．○○」からネット攻撃を受けている旨を通達する。

【００２１】この通達により、ルーター制御装置１０３では、ＩＰアドレス「２２３．○○．○○．○○」から送信されてくるデータを、回線ルーター１０１やインターネットルーター１０２で破棄させるように制御する。ルーター制御装置１０３の制御の結果、インターネット１３０上のＩＰアドレス「２２３．○○．○○．○○」から送信されてくるデータは、ユーザーＡ１１０に到達することが無く、Ｗｅｂサーバー１１１に対するネット攻撃は解消されることになる。

9

【００２２】以下、本発明の通信状態制御方法に関して、図３のフローチャートを用いて説明する。まず、トラフィック測定装置１１５がネットワーク１１３における通信状態を測定し（ステップＳ２）、測定した通信状態をトラフィック監視装置１１６が判断する（ステップＳ３）。これらは、所定の一定時間毎に行う（ステップＳ１）。この判定では、自身のネットワーク１１３の例えばＷｅｂサーバー１１１に対する特定のＩＰアドレスからのデータ量が、規定値を超えたかどうかを判定する。ステップＳ３の判定で、特定のＩＰアドレスからのデータ量が規定値を超えたと判定した場合、トラフィック監視装置１１６は、ルーター制御装置１０３に対して、特定のＩＰアドレスからの攻撃が、ＩＰアドレス「１０．ＸＸ．ＸＸ．ＸＸ」のＷｅｂサーバー１１１に対して発生したことを通知する（ステップＳ４）。

【００２３】トラフィック監視装置１１６から攻撃発生の通知を受けたルーター制御装置１０３は、回線ルーター１０１およびインターネットルーター１０２の動作を制限し、指定されたＩＰアドレスからのデータを破棄させる。この後、ルーター制御装置１０３は、破棄しているデータ量を監視し（ステップＳ７）、単位時間あたりの破棄データ量が規定値以下となったら、回線ルーター１０１およびインターネットルーター１０２の動作制限を解除する（ステップＳ８）。これらは、一定時間毎に行う（ステップＳ６）。

【００２４】なお、上記実施の形態では、トラフィック測定装置１１５で測定したネットワーク１１３を通過するデータの発信元ＩＰアドレスと発信先ＩＰアドレスとデータ量とをもとに、ユーザーのサーバーに対する攻撃を判断するようにしたが、これに限るものではない。トラフィック監視装置１１６で、Ｗｅｂサーバー１１１やメールサーバー１１２から、図４（ａ）に示すような、ネットワーク１１３に対して送信されてきたデータ量とこのデータの送信元などの情報、加えて、図４（ｂ）に示すような、各サーバーにおける単位時間あたりのＣＰＵ稼働率，主メモリ使用率，一定時間あたりの接続数（総トラフィック），単位時間あたりの通信量（トラフィック）を取得し、これら情報をもとに判断をするようにしてもよい。通信量の取得は、例えば、サーバーがネットワークに接続するためのインターフェース（ＮＩＣ）を通過している通信量を、各サーバーから取得するようにすればよい。

【００２５】例えば、上記ＣＰＵの稼働率と主メモリの使用率とサーバーに対する単位時間あたりのリクエスト数とサーバーに対する単位時間あたりの通信量とのいずれもが、図４（ｃ）に示すような予め設定されている規定値を超えたら、ネット攻撃を受けていると判定するようにしてもよい。この判定の場合、ネット攻撃を受けていると判定した時点においてアクセスしている送信元のＩＰアドレスが、ネット攻撃をしている攻撃元とし、トラフィック監視装置１１６は、この情報をルーター制御装置１０３に送信する。この結果、ルーター制御装置１０３は、回線ルーター１０１とインターネットルーター１０２とを制御し、上記ＩＰアドレスからの送信データを破棄させる。

10

【００２６】また、上記実施の形態では、トラフィック監視装置１１６で、ネット攻撃の発生有無を判定したが、これに限るものではなく、ルーター制御装置１０３でネット攻撃の発生有無を判定してもよい。この場合、トラフィック監視装置１１６は、トラフィック測定装置１１５が測定した結果や、トラフィック監視装置１１６が取得した情報を、ルーター制御装置１０３に送信し、トラフィック監視装置１１６から送られてきた情報をもとに、ルーター制御装置１０３が判定とルーター制御を行う。

【００２７】ルーター制御装置１０３が判定を行う場合に関して、図５のフローチャートを用いて説明する。まず、トラフィック測定装置１１５がネットワーク１１３における通信状態を測定し（ステップＳ５２）、測定した通信状態をトラフィック監視装置１１６が、ルーター制御装置１０３に送信する（ステップＳ５３）。次いで、データを受信したルーター制御装置１０３は、受け取った通信状態からネット攻撃の有無を判定する（ステップＳ５３）。これらは、一定時間毎に行う（ステップＳ５１）。この判定では、通信状態を送信してきたユーザーＡ１１０のネットワーク１１３のＷｅｂサーバー１１１に対する特定のＩＰアドレスからのデータ量が、規定値を超えたかどうかを判定する。

【００２８】ステップＳ５３の判定で、特定のＩＰアドレスからのデータ量が規定値を超えたと判定した場合、ルーター制御装置１０３は、回線ルーター１０１およびインターネットルーター１０２の動作を制限し、規定値を超えたデータ量を送信してきたＩＰアドレスからのデータを破棄させる（ステップＳ５５）。この後、ルーター制御装置１０３は、破棄しているデータ量を監視し（ステップＳ５７）、単位時間あたりの破棄データ量が規定値以下となったら、回線ルーター１０１およびインターネットルーター１０２の動作制限を解除する（ステップＳ５８）。これらは、一定時間毎に行う（ステップＳ５６）。

【００２９】

【発明の効果】以上説明したように、本発明によれば、一定量以上のデータを送信してきた送信元からのデータの送信が、ＩＳＰにおいて破棄されるので、大量のデータを送信してくる不正アクセスから、ＩＳＰに接続されているユーザーのサーバーを守れるという優れた効果が得られる。

【図面の簡単な説明】

【図１】　本発明の実施の形態における通信状態制御システムの構成を示す構成図である。

11

【図２】　トラフィック測定装置の測定結果の一例を示す図である。

【図３】　本発明の実施の形態における通信状態制御方法を示すフローチャートである。

【図４】　トラフィック監視装置の取得したデータの一例を示す図である。

【図５】　本発明の他の形態における通信状態制御方法示すフローチャートである。

【図６】　従来のＩＳＰを介してインターネットに接続＊

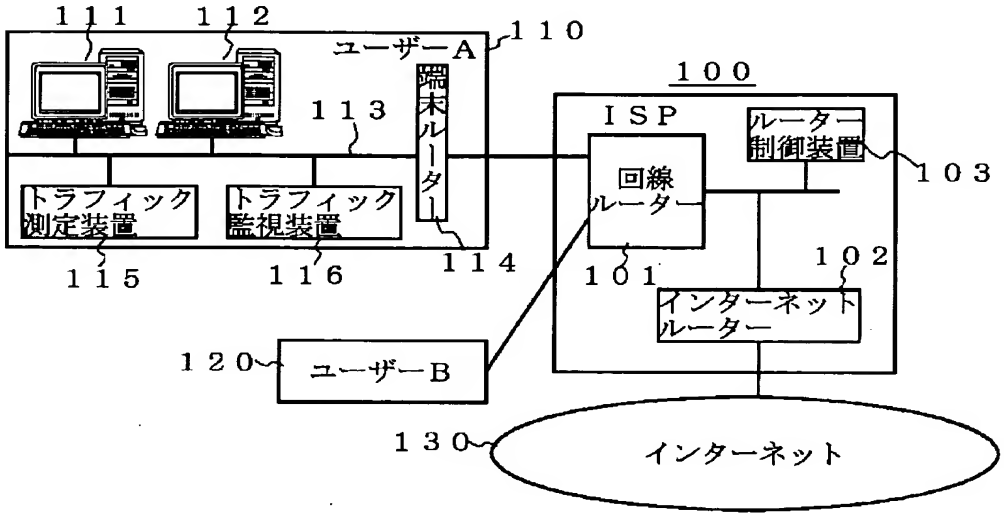
12

＊する形態を示す構成を示す構成図である。

【符号の説明】

１００…ＩＳＰ（Internet Service Provider）、１０１…回線ルーター、１０２…インターネットルーター、１０３…ルーター制御装置、１１０…ユーザーＡ、１１１…Ｗｅｂサーバー、１１２…メールサーバー、１１３…ネットワーク、１１４…端末ルーター、１１５…トラフィック測定装置、１１６…トラフィック監視装置、１２０…ユーザーＢ、１３０…インターネット。

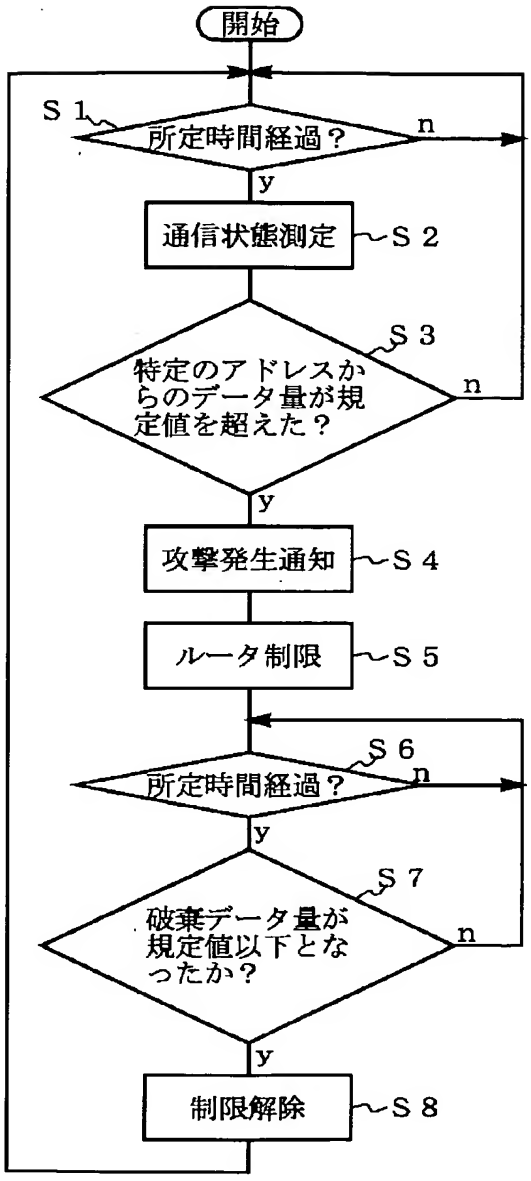
【図１】



【図２】

アクセス時刻	送信元ＩＰアドレス	受信先ＩＰアドレス	データ量	・・・
2000/4/18 18:45:00	10.XX.XX.XX	233.XX.XX.XX	○○○	・・・
	11.XX.XX.XX	234.XX.XX.XX	○○○	・・・
	・・・	・・・	・・・	・・・
	・・・	・・・	・・・	・・・
	・・・	・・・	・・・	・・・
2000/4/18 18:45:02	10.XX.XX.XX	223.XX.XX.XX	・・・	・・・
	11.XX.XX.XX	224.XX.XX.XX	・・・	・・・
	・・・	・・・	・・・	・・・
	・・・	・・・	・・・	・・・
	・・・	・・・	・・・	・・・

【図３】


開始
S 1
所定時間経過？
n
y
通信状態測定
S 2
S 3
特定のアドレスからのデータ量が規定値を超えた？
n
y
攻撃発生通知
S 4
ルータ制限
S 5
S 6
所定時間経過？
n
y
S 7
破棄データ量が規定値以下となったか？
n
y
制限解除
S 8

【図４】

（ａ）

アクセス時刻	送信元ＩＰアドレス	データ量	ＤＮＳ情報	・・・	・・・
2000/4/18 18:45:00	234.XX.XX.XX	○○○	□□□	・・・	・・・
	233.XX.XX.XX	○○○	□□□	・・・	・・・
	・・・	・・・	・・・	・・・	・・・
	・・・	・・・	・・・	・・・	・・・
	・・・	・・・	・・・	・・・	・・・
2000/4/18 18:45:02	234.XX.XX.XX	△△△	・・・	・・・	・・・
	233.XX.XX.XX	△△△	・・・	・・・	・・・
	・・・	・・・	・・・	・・・	・・・
	・・・	・・・	・・・	・・・	・・・
	・・・	・・・	・・・	・・・	・・・

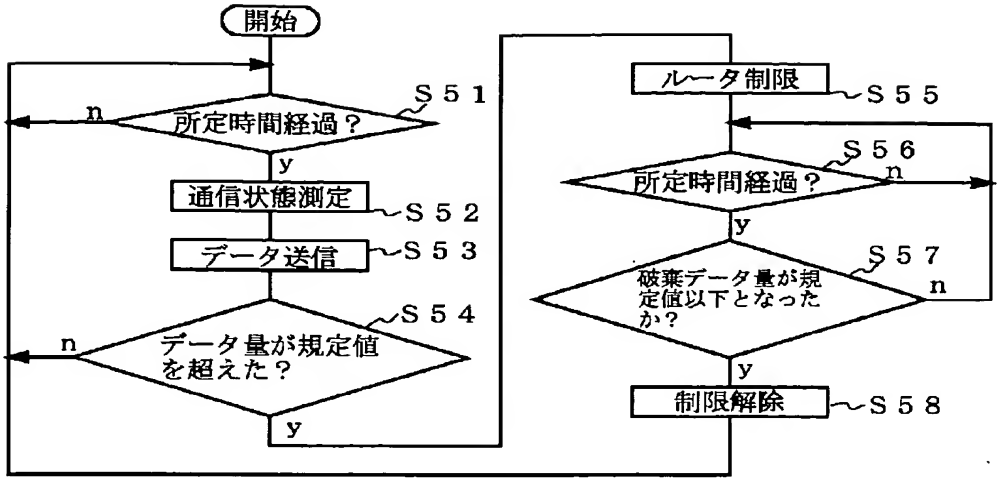
（ｂ）

監視項目／対象	単位時間あたりのＣＰＵ稼働率	単位時間あたりのメモリ稼働率	一定時間あたりの総トラフィック	単位時間あたりのトラフィック
Ｗｅｂサーバ	２５	１５	２２５５５０	１８５
端末ルータ	５０	５０	１２５８８２２	３５２
・	・	・	・	・
・	・	・	・	・
・	・	・	・	・
・	・	・	・	・

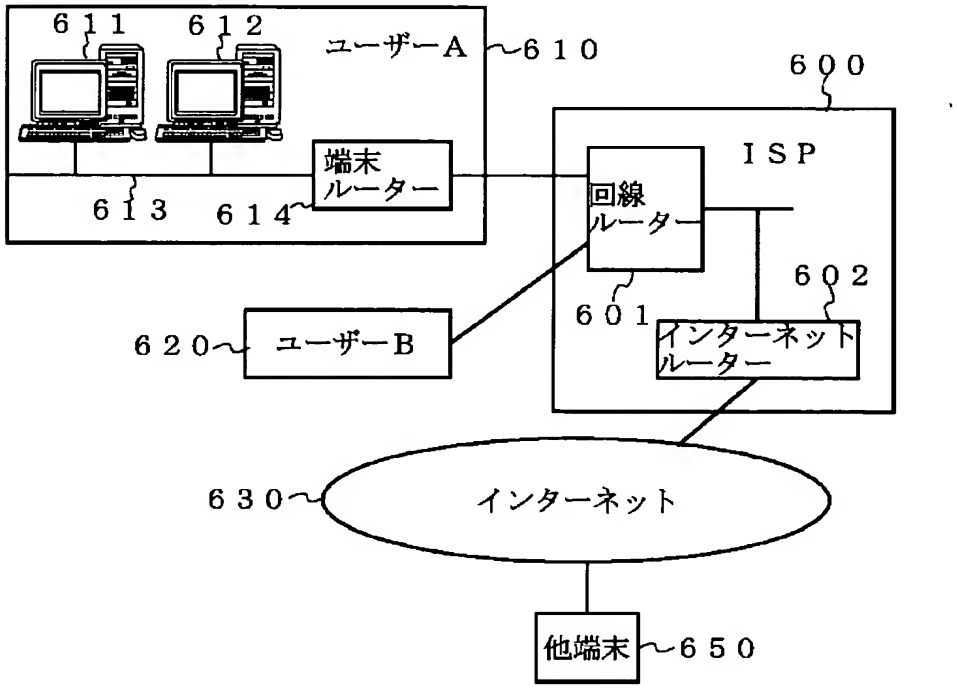
（ｃ）

	Ｗｅｂサーバ	端末ルーター	・	・
単位時間あたりのＣＰＵ稼働率	８５	８２	・	・
単位時間あたりのメモリ稼働率	９８	９８	・	・
一定時間あたりの総トラフィック	３００００００	２５０００００	・	・
単位時間あたりのトラフィック	５００	５０００	・	・
一定、単位時間あたりのﾄﾗﾌｨｯｸ(特定送信元IPｱﾄﾞﾚｽ)	１２００００	５０００００	・	・
	３８０	３５００	・	・
・	・	・	・	・

【図５】


開始
所定時間経過？
S５１
n
y
通信状態測定
S５２
データ送信
S５３
データ量が規定値を超えた？
S５４
n
y
ルータ制限
S５５
S５６
所定時間経過？
n
y
破棄データ量が規定値以下となったか？
S５７
n
y
制限解除
S５８

【図６】


６１１
６１２
ユーザーA
６１０
６００
ISP
端末ルーター
６１３
６１４
回線ルーター
６０２
６０１
インターネットルーター
６２０
ユーザーB
６３０
インターネット
他端末
６５０